SON-2321 PATENT APPLICATION

2131
#6/A
6-11-03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of

Hideaki WATANABE et al. Group Art: 2131

Serial No. 10/040,436 Examiner: Unknown

Filed: January 9, 2002 Attorney Docket No.: SON-2321

Title: PUBLIC KEY CERTIFICATE ISSUING SYSTEM, PUBLIC KEY CERTIFICATE ISSUING METHOD, INFORMATION PROCESSING APPARATUS, INFORMATION RECORDING MEDUIM, AND PROGRAM STORAGE MEDUIM

PRELIMINARY AMENDMENT

Commissioner of Patents
Washington, DC 20231

Sir:

Prior to the initial examination, please amend the above-identified application as follows:

IN THE SPECIFICATION:

Please rewrite the following paragraphs as set forth below in clean form. Additionally, in accordance with 37 CFR 1.121(b)(1)(iii), the amended paragraphs are set forth in a marked-up version in the pages attached to this Amendment.

Beginning at page 3, line 10:

Unlike a so-called common key cryptosystem in which a common key is used for both encryption and decryption, the public key cryptosystem is advantageous in the management of keys because only one particular person may have the private key, which must be kept secret. However, the public key cryptosystem is slower than the common key cryptosystem in data

10/640,436 ram 10/27/04

processing speed and therefore often used for such applications requiring only small amounts of data as the delivery of a private key and the execution of digital signature. A typical public key cryptosystem is RSA (Rivest-Sharmir-Adleman). RSA uses a product of very large two prime numbers (for example, 150 digits) to make it difficult to perform factorization (and discrete logarithm) on the product.

A1 cancel.

Kam 10/27/04

Beginning at page 4, line 11 5:

While RSA cryptosystem based on factorization into prime factors (and discrete logarithm) has sub-exponential decryption, elliptic curve logarithm is considered to have only exponential decryption. While the key size of RSA cryptosystem based on discrete logarithmic problem is 512, 1024, or 2048 bits, the key size of ECC is 160, 192, or 224 bits, which provides generally the same level of security as that of RSA with a shorter key size, resulting in enhanced processing speed.

A2

Beginning at page 5, line 9:

The following describes a public key certificate with reference to FIG. 1. A public key certificate is issued by a certificate authority (CA) or an issuer authority (IA) in the public key cryptosystem. The public key certificate is prepared by a user submitting his ID and public key to a certificate authority and this certificate authority then attaching its ID, validity and signature to the information submitted by the user.

A3

Beginning at page 10, line 4:

In order for the ECC device 23 and the RSA device 33 shown in FIG. 2 to verify the validity of the public key certificate of each other, a configuration must be used where the ECC device 23 and the RSA device 33 send the public key certificates received from each other to the ECC registration authority 22 and the RSA registration authority 32 and then to the ECC certificate authority (ECC-CA) 21 and the RSA certificate authority (RSA-CA) 31 respectively. Inquiries are executed between the ECC certificate authority (ECC-CA) 21 and the RSA

A4